

ABSTRACT

A method for distributing encryption keys in WLAN, said method combines key distribution process with authentication process of the mobile hosts and utilizes an authentication server or a wireless gateway to manage key distribution, so that mobile hosts can roam in a scope larger than the coverage area of the key management server. Because the key distribution doesn't involve transmitting the key, which is not encrypted via the air interface, the method ensures the key is safe. In addition, said method doesn't depend on specific authentication modes, so it can be used under different kinds of WLAN protocols. Finally, because AP doesn't need to manage user information, the method simplifies AP structure, and thus lowers the cost.